PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-187008
(43)Date of publication of application : 09.07.1999

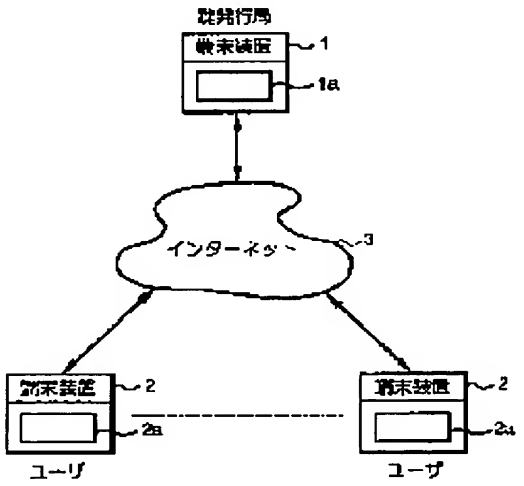
(51)Int.Cl. H04L 9/08
G09C 1/00
G09C 1/00

(21)Application number : 09-348289
(22)Date of filing : 17.12.1997

(71)Applicant : CARD CALL SERVICE KK
(72)Inventor : BABA YOSHIMI

(54) DELIVERING METHOD FOR CRYPTOGRAPHIC KEY

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a delivering method for cryptographic key improved in versatility or convenience by safely and easily delivering a cryptographic key for cryptographic communication to the user of a cryptographic communication system by communication through an internet while securing its secrecy.
SOLUTION: Communication is enabled though an internet 3 between terminal equipment 1 of a key issue station and terminal equipment 2 of the user while using a hyper text transfer protocol(HTTP), a disclosed key based on an Elgamal code is transmitted from the terminal equipment 1 through the internet 3 to the terminal equipment 2. Next, random number data generated by the terminal equipment 2 are enciphered by the disclosed key, transmitted to the terminal equipment 1 and deciphered by the terminal equipment 2 so that common random number data are shared between both the terminal equipment 1 and 2. Next, these random number data are used as the key of a common key system, the cryptographic key for user generated by the terminal equipment 1 is enciphered and transmitted to the terminal equipment 2 and that key is deciphered while using the random number data held at the terminal equipment 1.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－187008

(43)公開日　平成11年(1999)７月９日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ
Ｇ０９Ｃ　1/00	６３０	Ｇ０９Ｃ　1/00	６３０Ｂ
	６６０		６６０Ｅ

審査請求　未請求　請求項の数７　ＯＬ　（全 11 頁）

(21)出願番号　特願平9－348289

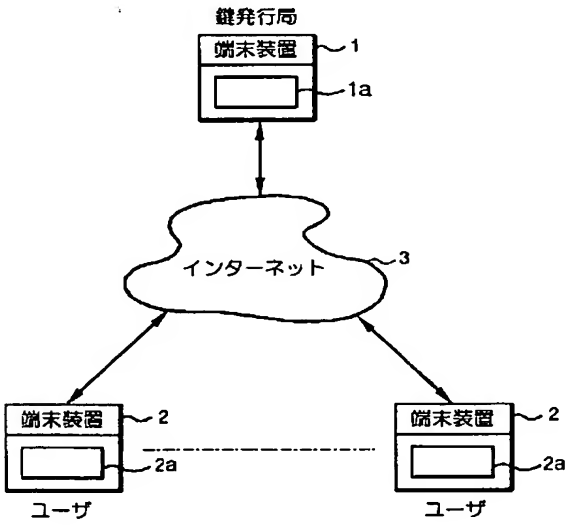
(22)出願日　平成９年(1997)12月17日

(71)出願人　595095135
カード・コール・サービス株式会社
東京都渋谷区道玄坂１丁目22番７号
(72)発明者　馬場　芳美
千葉県船橋市宮本８丁目10番３号
(74)代理人　弁理士　佐藤　辰彦　（外１名）

(54)【発明の名称】　暗号鍵の配送方法

(57)【要約】
【課題】暗号通信のための暗号鍵を、その機密性を確保しつつインターネットを介した通信により安全且つ簡易に暗号通信システムのユーザに配送することができ、汎用性や利便性に優れた暗号鍵の配送方法を提供する。
【解決手段】鍵発行局の端末装置１とユーザの端末装置２との間でＨＴＴＰを使用してインターネット３を介して通信可能としておき、端末装置１から端末装置２にエルガマル暗号による公開鍵をインターネット３を介して送信する。次いで、端末装置２で生成した乱数データを公開鍵で暗号化して端末装置１に送信し、それを端末装置２で復号化することで両端末装置１，２で共通の乱数データを共有する。次いで、この乱数データを共通鍵方式の鍵として使用して端末装置１で生成したユーザ用の暗号鍵を暗号化して端末装置２に送信し、それを端末装置１で保持した乱数データを用いて復号化する。

FIG. 1



1

【特許請求の範囲】

【請求項１】暗号通信システムのユーザ間で暗号通信を行う際に各ユーザが使用する暗号鍵を該暗号通信システムの鍵発行局から各ユーザに配送する方法であって、

あらかじめ各ユーザ及び鍵発行局がそれぞれ所持する端末装置に、データの一回の通信毎にインターネットの不特定の通信経路を介して通信を行うインターネット通信手段を用意しておき、

ユーザがその端末装置から鍵発行局の端末装置に前記暗号鍵の配送を要求したとき、該鍵発行局の端末装置において公開鍵方式による暗号通信のための暗号化用の公開鍵及び復号化用の秘密鍵を生成して保持し、その公開鍵及び秘密鍵のうち、公開鍵を該鍵発行局の端末装置からユーザの端末装置に前記インターネット通信手段を介して送信する工程と、

前記公開鍵を受信したユーザの端末装置において、該ユーザがその端末装置の所定の操作を行うことにより該ユーザに固有の乱数データを生成して保持した後、該乱数データを前記公開鍵により暗号化し、その暗号化した乱数データを該ユーザの端末装置から鍵発行局の端末装置に前記インターネット通信手段を介して送信する工程と、

前記暗号化された乱数データを受信した鍵発行局の端末装置において、その暗号化された乱数データを前記秘密鍵により復号化して保持する工程と、

前記復号化した乱数データを保持した鍵発行局の端末装置において、ユーザの前記暗号鍵を生成した後、前記乱数データを共通鍵方式による暗号通信のための鍵として用いて該暗号鍵を暗号化し、その暗号化した暗号鍵を該鍵発行局の端末装置からユーザの端末装置に前記インターネット通信手段を介して送信する工程と、

前記暗号化された暗号鍵を受信したユーザの端末装置において、該端末装置に保持した前記乱数データを前記共通鍵方式による鍵として用いて前記暗号化された暗号鍵を復号化して保持する工程とから成ることを特徴とする暗号鍵配送方法。

【請求項２】暗号通信システムのユーザ間で暗号通信を行う際に各ユーザが使用する暗号鍵を該暗号通信システムの鍵発行局から各ユーザに配送する方法であって、

あらかじめ各ユーザ及び鍵発行局がそれぞれ所持する端末装置に、データの一回の通信毎にインターネットの不特定の通信経路を介して通信を行うインターネット通信手段を用意しておき、

ユーザがその端末装置から鍵発行局の端末装置に前記暗号通信システムへの加入の申し込みしたとき、該鍵発行局の端末装置において公開鍵方式による暗号通信のための暗号化用の公開鍵及び復号化用の秘密鍵を生成して保持し、その公開鍵及び秘密鍵のうち、公開鍵を該鍵発行局の端末装置からユーザの端末装置に前記インターネット通信手段を介して送信する工程と、

2

前記公開鍵を受信したユーザの端末装置において、該ユーザがその端末装置の所定の操作を行うことにより該ユーザに固有の乱数データを生成して保持すると共に前記鍵発行局が該ユーザを特定するための該ユーザの個人情報を該端末装置に入力した後、該乱数データ及び個人情報を前記公開鍵により暗号化し、その暗号化した乱数データ及び個人情報を該ユーザの端末装置から鍵発行局の端末装置に前記インターネット通信手段を介して送信する工程と、

前記暗号化された乱数データ及び個人情報を受信した鍵発行局の端末装置において、その暗号化された乱数データ及び個人情報を前記秘密鍵により復号化して保持する工程と、

前記復号化した乱数データ及び個人情報を保持した鍵発行局の端末装置において、該個人情報に係わるユーザの前記暗号鍵を生成した後、前記復号化した乱数データを共通鍵方式による鍵として用いて該暗号鍵を暗号化し、その暗号化した暗号鍵を鍵発行局の端末装置からユーザの端末装置に前記インターネット通信手段を介して送信する工程と、

前記暗号化された暗号鍵を受信したユーザの端末装置において、該端末装置に保持した前記乱数データを前記共通鍵方式による鍵として用いて前記暗号化された暗号鍵を復号化して保持する工程とから成ることを特徴とする暗号鍵配送方法。

【請求項３】前記暗号鍵は前記鍵発行局の端末装置において前記ユーザの個人情報に基づき生成することを特徴とする請求項２記載の暗号鍵配送方法。

【請求項４】前記公開鍵方式による暗号通信はエルガマル（Elgamal)暗号を使用することを特徴とする請求項１乃至３のいずれかに記載の暗号鍵配送方法。

【請求項５】前記公開鍵方式による公開鍵及び秘密鍵は、該公開鍵を前記鍵発行局の端末装置からユーザの端末装置に送信する都度生成することを特徴とする請求項４記載の暗号鍵配送方法。

【請求項６】前記ユーザの端末装置における前記乱数データの生成は、該ユーザによる所定の入力操作のタイミングに基づき生成することを特徴とする請求項１乃至５のいずれかに記載の暗号鍵配送方法。

【請求項７】前記暗号鍵は、これに通信相手側のユーザの識別子を作用させることにより該通信相手側のユーザとの暗号通信用の共通鍵を生成するアルゴリズムから成ることを特徴とする請求項１乃至６のいずれかに記載の暗号鍵配送方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号通信システムのユーザ間で暗号通信を行うために使用する暗号鍵を各ユーザに配送する方法に関する。

【０００２】

【従来の技術】暗号通信システムのユーザ間で暗号通信を行う手法としては、公開鍵方式や共通鍵方式が知られており、このうち、公開鍵方式は、各ユーザがデータの暗号化のための鍵を公開鍵として他者に公開すると共に、復号化のための鍵を秘密鍵として秘密裏に所持するもので、所謂、ＲＳＡ暗号やエルガマル（Elgamal)暗号がこの方式の範疇に属するものである。この場合、各ユーザ毎の公開鍵及び秘密鍵は暗号通信システムの鍵発行局で生成され、該鍵発行局は、各ユーザ毎の公開鍵の管理や各ユーザへの秘密鍵の配送を行う。そして、ユーザ間の暗号通信に際しては、送信側のユーザが受信側のユーザの公開鍵を用いてデータを暗号化して送信し、それを受信側のユーザが自身の秘密鍵を用いて復号化する。

【０００３】また、共通鍵方式は、暗号通信を行うユーザ同士が、暗号及び復号化のための共通鍵を共有するもので、この方式では、例えばRolf Blom による論文「NON-PUBLIC KEY DISTRIBUTION ／Advance in Cryptology: Proceedings of CRYPTO '82／Plenum Press 1983,pp.231-236」、同じくRolf Blom による論文「An OptimalClass of Symmetric Key Generation Systems ／Advances in Cryptology:EUROCRYPT '84／Springer LNCS 209, 1985,pp.335-338」、あるいは特公平５－４８９８０号公報もしくは米国特許第５０１６２７６号に見られるように、通信相手側の氏名等の識別子を作用させることでその通信相手側との共通鍵を生成するアルゴリズムを、各ユーザに固有の秘密鍵として各ユーザ毎に鍵発行局で生成し、それを鍵発行局から各ユーザに配送しておくようにしたものが知られている。この方式では、ユーザ間の暗号通信に際しては、各ユーザがそれぞれ自己の端末装置において、通信相手側の識別子を自己の秘密鍵に作用させることで、通信相手側のユーザとの共通鍵を生成し、その共通鍵によりデータの暗号・復号化を行って暗号通信を行う。

【０００４】ところで、この種の暗号通信システムでは、前述の公開鍵方式における秘密鍵や共通鍵方式における秘密鍵というような暗号鍵は、極めて高度の機密性を要求されるものである一方、各ユーザに鍵発行局から配送する必要がある。従って、上記のように高度の機密性を要求される暗号鍵をいかにして安全に各ユーザに配付するかが重要な課題となる。

【０００５】一方、近年の情報通信分野では、インターネットの利用が急速に普及しており、このような状況下では、暗号通信システムの汎用性あるいは利便性を考慮すると、上記のような暗号鍵の配送もインターネットを介した通信により行うことが望まれる。

【０００６】しかるに、インターネットは、誰もが自由に利用できるものであるため、上記のように高度の機密性を要求される暗号鍵をインターネットを経由して配送することは機密性の確保が困難であると考えられている。

【０００７】このため、従来は、上記のような暗号鍵の配送は、一般に、この暗号鍵のデータを記録したフロッピディスク等の物理的な記録媒体を各ユーザに配送することで行われている。

【０００８】しかしながら、このような暗号鍵の配送手法では、コスト的に不利なものとなると共に、ユーザが暗号通信システムへの加入を申し込んでから、暗号鍵を受け取って実際に暗号通信システムを利用することができるようになるまでに時間がかかったりして、利便性に欠けるものとなっていた。

【０００９】尚、暗号鍵をある者から他者に配送する場合、その両者間であらかじめ合言葉等を取り決めて共用しておき、暗号鍵の送り手側及び受けて側がそれぞれ互いに共用した合言葉等から所定の方式でＤＥＳ（Data Encryption Standard）の鍵を生成すると共に、送り手側が配送しようとする暗号鍵を上記のＤＥＳ鍵を使用して暗号化して受け手側に与え、それを受け手側が上記のＤＥＳ鍵を使用して復号化することで、該暗号鍵を安全に配送し得るようにしたものを、RSA Laboratories（ＲＳＡ研究所）がインターネットのホームページ（http://www.rsa.com/rsalab ）上で公表している（題名：「PKCS #5／Password-Based Encryption Standard／An RSA Laboratories Technical Note／Version 1.5 ／Revised November 1,1993 」）。この手法では、暗号鍵を暗号化して配送するため、一見すると、該号鍵をインターネット等の通信によって安全に配送することができるように見える。しかるに、この手法では、暗号鍵の配送の安全性を確保する上では、前記合言葉等を暗号鍵の送り手側と受け手側とで安全に（第三者に判らないように）取り決めておかなければならない。従って、前記合言葉等をいかにして両者間で安全に授受するかが問題となってしまい、その授受をフロッピディスク等の物理的な記録媒体で行うようにすれば、前述と同様の不都合を生じてしまう。

【００１０】

【発明が解決しようとする課題】本発明はかかる背景に鑑み、暗号通信のための暗号鍵を、その機密性を確保しつつインターネットを介した通信により安全且つ簡易に暗号通信システムのユーザに配送することができ、汎用性や利便性に優れた暗号鍵の配送方法を提供することを目的とする。

【００１１】

【課題を解決するための手段】本発明の暗号鍵の配送方法の第１の態様はかかる目的を達成するために、暗号通信システムのユーザ間で暗号通信を行う際に各ユーザが使用する暗号鍵を該暗号通信システムの鍵発行局から各ユーザに配送する方法であって、あらかじめ各ユーザ及び鍵発行局がそれぞれ所持する端末装置に、データの一回の通信毎にインターネットの不特定の通信経路を介して通信を行うインターネット通信手段を用意しておき、

ユーザがその端末装置から鍵発行局の端末装置に前記暗号鍵の配送を要求したとき、該鍵発行局の端末装置において公開鍵方式による暗号通信のための暗号化用の公開鍵及び復号化用の秘密鍵を生成して保持し、その公開鍵及び秘密鍵のうち、公開鍵を該鍵発行局の端末装置からユーザの端末装置に前記インターネット通信手段を介して送信する工程と、前記公開鍵を受信したユーザの端末装置において、該ユーザがその端末装置の所定の操作を行うことにより該ユーザに固有の乱数データを生成して保持した後、該乱数データを前記公開鍵により暗号化し、その暗号化した乱数データを該ユーザの端末装置から鍵発行局の端末装置に前記インターネット通信手段を介して送信する工程と、前記暗号化された乱数データを受信した鍵発行局の端末装置において、その暗号化された乱数データを前記秘密鍵により復号化して保持する工程と、前記復号化した乱数データを保持した鍵発行局の端末装置において、ユーザの前記暗号鍵を生成した後、前記乱数データを共通鍵方式による暗号通信のための鍵として用いて該暗号鍵を暗号化し、その暗号化した暗号鍵を該鍵発行局の端末装置からユーザの端末装置に前記インターネット通信手段を介して送信する工程と、前記暗号化された暗号鍵を受信したユーザの端末装置において、該端末装置に保持した前記乱数データを前記共通鍵方式による鍵として用いて前記暗号化された暗号鍵を復号化して保持する工程とから成ることを特徴とする。

【００１２】かかる本発明によれば、ユーザがその端末装置から鍵発行局の端末装置にアクセスして前記暗号鍵の配送の要求を行うと、鍵管理局の端末装置において、公開鍵方式による暗号化用の公開鍵及び復号化用の秘密鍵が生成され、これらの公開鍵及び秘密鍵のうち、公開鍵が鍵管理局の端末装置からユーザの端末装置にインターネット通信手段を介して与えられる。そして、この公開鍵を受け取ったユーザの端末装置では、該ユーザがその端末装置の所定の操作により生成して保持した該ユーザに固有の乱数データが該公開鍵によって暗号化され、その暗号化された乱数データがユーザの端末装置から鍵管理局の端末装置にインターネット通信手段を介して送信される。そして、上記のように暗号化された乱数データを受け取った鍵発行局の端末装置では、前記秘密鍵により該乱数データを復号化し、ユーザ側の端末装置で保持されている乱数データと共通の乱数データを取得する。これによりユーザと鍵発行局とは、共通鍵方式の暗号通信の鍵として使用し得る乱数データを共有することとなる。

【００１３】このとき、前記公開鍵と、この公開鍵により暗号化された乱数データとは個別にインターネット通信手段を介して通信されるため、それらのインターネット上での通信経路は不特定で一般には同一の通信経路を通らない。このため、前記公開鍵や、これにより暗号化された乱数データを第三者が個別に獲得することがあっても、それらをひとまとめに獲得することは極めて困難である。従って、例えば暗号化された乱数データを第三者が獲得しても、それがどのような暗号手法で暗号化されたものかが判らない。さらには、該乱数データはユーザ自身の端末装置の操作によって生成した該ユーザに固有のものであるため、元々、第三者には予測がつきにくいものとなっていると共に、前記公開鍵により暗号化されて送信される。これにより、前記公開鍵により暗号化された乱数データを第三者が解読することは難しものとなって、該乱数データが安全にユーザから鍵発行局に受け渡される。

【００１４】次に、上記のように乱数データを復号化して取得した鍵発行局の端末装置では、ユーザに配送すべき前記暗号鍵を生成した後、その暗号鍵を、前記復号化した乱数データを共通鍵方式による暗号通信の鍵として用いて暗号化し、その暗号化した暗号鍵を鍵発行局の端末装置からユーザの端末装置にインターネット通信手段を介して送信する。そして、この暗号化された暗号鍵を受け取ったユーザの端末装置では、その端末装置に保持されている前記乱数データを共通鍵方式の鍵として用いて、暗号化された暗号鍵を復号化し、これにより所望の暗号鍵を取得する。

【００１５】このとき、鍵発行局の端末装置からユーザの端末装置に送信される暗号化された暗号鍵を第三者が個別に獲得することがあっても、その暗号鍵の暗号化の鍵として使用された前記乱数データは元々、第三者には予測がつきにくく、また、該乱数データを鍵として用いる暗号通信は、鍵発行局の端末装置からユーザの端末装置に前記暗号鍵を通信する際にだけ行われるので、該乱数データを鍵として暗号化された前記暗号鍵を、それを獲得した第三者が解読することは極めて困難である。しかも、鍵発行局からユーザへの前記暗号鍵の暗号通信に先立って行われる前記公開鍵方式による乱数データの暗号通信と、この乱数データを鍵とする前記共通鍵方式による前記暗号鍵の暗号通信とは、各別にインターネット上の不特定の通信経路を介して行われるため、それらの暗号化された乱数データと暗号化された暗号鍵とをひとまとめに第三者が取得することも難しい。従って、仮に第三者が、前記公開鍵により暗号化された乱数データを取得してそれを解読したとしても、その乱数データを鍵として暗号化された前記暗号鍵を取得することは難しい。

【００１６】これにより、前記暗号鍵がインターネットを介して各ユーザに安全に配送されることとなる。さらに、該暗号鍵の通信は、共通鍵方式による暗号通信により行うため、その暗号鍵の暗号化や復号化を迅速に効率よく行うことができる。

【００１７】よって、本発明によれば、暗号通信のための暗号鍵を、その機密性を確保しつつインターネットを介した通信により安全且つ簡易に暗号通信システムのユ

ーザに配送することができ、汎用性や利便性に優れた暗号鍵の配送方法を提供できる。

【００１８】また、本発明のより具体的な第２の態様は、暗号通信システムのユーザ間で暗号通信を行う際に各ユーザが使用する暗号鍵を該暗号通信システムの鍵発行局から各ユーザに配送する方法であって、あらかじめ各ユーザ及び鍵発行局がそれぞれ所持する端末装置に、データの一回の通信毎にインターネットの不特定の通信経路を介して通信を行うインターネット通信手段を用意しておき、ユーザがその端末装置から鍵発行局の端末装置に前記暗号通信システムへの加入の申し込みしたとき、該鍵発行局の端末装置において公開鍵方式による暗号通信のための暗号化用の公開鍵及び復号化用の秘密鍵を生成して保持し、その公開鍵及び秘密鍵のうち、公開鍵を該鍵発行局の端末装置からユーザの端末装置に前記インターネット通信手段を介して送信する工程と、前記公開鍵を受信したユーザの端末装置において、該ユーザがその端末装置の所定の操作を行うことにより該ユーザに固有の乱数データを生成して保持すると共に前記鍵発行局が該ユーザを特定するための該ユーザの個人情報を該端末装置に入力した後、該乱数データ及び個人情報を前記公開鍵により暗号化し、その暗号化した乱数データ及び個人情報を該ユーザの端末装置から鍵発行局の端末装置に前記インターネット通信手段を介して送信する工程と、前記暗号化された乱数データ及び個人情報を受信した鍵発行局の端末装置において、その暗号化された乱数データ及び個人情報を前記秘密鍵により復号化して保持する工程と、前記復号化した乱数データ及び個人情報を保持した鍵発行局の端末装置において、該個人情報に係わるユーザの前記暗号鍵を生成した後、前記復号化した乱数データを共通鍵方式による鍵として用いて該暗号鍵を暗号化し、その暗号化した暗号鍵を鍵発行局の端末装置からユーザの端末装置に前記インターネット通信手段を介して送信する工程と、前記暗号化された暗号鍵を受信したユーザの端末装置において、該端末装置に保持した前記乱数データを前記共通鍵方式による鍵として用いて前記暗号化された暗号鍵を復号化して保持する工程とから成ることを特徴とするものである。

【００１９】かかる本発明では、ユーザがその端末装置から鍵発行局の端末装置にアクセスして該鍵発行局に前記暗号通信システムへの加入の申し込みしたとき、前述の本発明の第１の態様と同様に鍵発行局の端末装置からユーザの端末装置に前記公開鍵が受け渡された後、ユーザがその端末装置の所定の操作により生成した該ユーザに固有の乱数データと、該端末装置に入力したユーザの個人情報とが、該ユーザの端末装置において前記公開鍵により暗号化され、その暗号化された乱数データ及び個人情報が該ユーザの端末装置から鍵発行局の端末装置に前記インターネット通信手段を介して送信される。そして、この暗号化された乱数データ及び個人情報を受け取った鍵発行局の端末装置では、前記秘密鍵により復号化して保持する。これにより、鍵発行局側では、暗号通信システムに加入するユーザに暗号鍵を共通鍵方式の暗号通信により配送するための鍵として使用する乱数データと、該ユーザを特定するための該ユーザの個人情報とを取得することができることとなる。

【００２０】このとき、前述した第１の態様の場合と同様に、前記公開鍵の通信と、この公開鍵により暗号化された乱数データ及び個人情報の通信とは、前記インターネット通信手段によってインターネット上の不特定の通信経路を介して個別に行われ、また、乱数データ及び個人情報は公開鍵により暗号化されて通信されるため、第三者が、乱数データ及び個人情報を解読することは難しい。従って、上記乱数データ及び個人情報のユーザ側から鍵発行局側への受け渡しが安全に行われる。また、該個人情報は共通鍵方式で暗号・復号化されるため、その暗号化や復号化が迅速に行われる。

【００２１】このようにして鍵発行局側でユーザに固有の乱数データと個人情報とを取得した後には、該鍵発行局の端末装置において該個人情報に係わるユーザの前記暗号鍵が生成され、この暗号鍵が前記第１の態様と全く同様にして、前記乱数データを鍵として用いる共通鍵方式の暗号通信により、鍵発行局の端末装置からユーザの端末装置にインターネット通信手段を介して送信される。そして、ユーザの端末装置では、これに保持した乱数データを鍵として用いて、暗号化された暗号鍵を復号することで、所要の暗号化を取得する。

【００２２】このとき、前述の第１の態様について説明した通り、前記暗号鍵がインターネットを介して各ユーザに安全に配送されることとなる。さらに、該暗号鍵の通信は、共通鍵方式による暗号通信により行うため、その暗号鍵の暗号化や復号化を迅速に効率よく行うことができる。

【００２３】このような本発明の第２の態様によれば、暗号通信のための暗号鍵を、前記第１の態様と同様にその機密性を確保しつつインターネットを介した通信により安全且つ簡易に暗号通信システムのユーザに配送することができる他、鍵発行局側でユーザを特定するための該ユーザの個人情報を安全且つ効率よく該鍵発行局が受け取ることができるため、ユーザが暗号通信システムに加入するための手続処理を暗号鍵の配送を含めて安全且つ容易に行うことができ、暗号通信システムの汎用性や利便性を高めることができる。

【００２４】このような本発明の第２の態様は、特に前記暗号鍵を前記鍵発行局の端末装置において前記ユーザの個人情報に基づき生成する場合に効果的である。すなわち、この場合に前記暗号鍵を生成するために必要なユーザの個人情報は、前述のように安全且つ効率よくユーザ側から鍵発行局側に受け渡されるため、その個人情報に基づく暗号鍵も鍵管理局側で安全且つ効率よく生成す

ることができる。

【００２５】また、以上説明したような本発明の第１又は第２の態様では、前記公開鍵方式による暗号通信はエルガマル（Elgamal)暗号を使用することが好ましい。すなわち、該エルガマル暗号は、ＲＳＡ暗号等に比べてデータの暗号化や復号化のための処理が比較的短時間で済み、このため、前記乱数データの暗号化や復号化を効率よく行うことができる。そして、この場合、エルガマル暗号はＲＳＡ暗号に比べて多数の暗号データの収拾等による攻撃に対して安全強度が弱いとされているものの、本発明では、該エルガル暗号による暗号通信は、ユーザの端末装置から鍵発行局の端末装置に前記乱数データを送信する際にだけしか使用されないため、十分な安全性を確保することができる。

【００２６】そして、特に、前記公開鍵方式による公開鍵及び秘密鍵を、該公開鍵を前記鍵発行局の端末装置からユーザの端末装置に送信する都度生成するようにしたときには、前記エルガマル暗号による前記乱数データの通信は、基本的には、その通信の都度、異なる鍵を使用して該乱数データの暗号化及び復号化が行われることとなるため、安全性の強度をより高めることができる。この場合、安全性の強度は通常のＲＳＡ暗号以上のものとすることができる。

【００２７】また、本発明の第１又は第２の態様では、前記ユーザの端末装置における前記乱数データの生成は、該ユーザによる所定の入力操作のタイミングに基づき生成することが好ましい。このような乱数データの生成を行うことで、再現性に乏しく、しかも予測しにくい該ユーザに固有の乱数データを生成することができ、該乱数データを共通鍵方式の鍵として使用する前記暗号鍵の暗号通信の安全性をより高めることができる。

【００２８】尚、本発明では、前記暗号鍵は、例えばこれに通信相手側のユーザの識別子を作用させることにより該通信相手側のユーザとの暗号通信用の共通鍵を生成するアルゴリズムから成る。この場合、前記暗号鍵が配送された後に、ユーザ同士が暗号通信を行う際には、各ユーザが独自に、自身の暗号鍵に通信相手側のユーザの識別子を作用させるだけで、その通信相手側のユーザとの共通鍵を得ることができるので、その共通鍵を用いた暗号通信を簡単に行うことができる。

【００２９】

【発明の実施の形態】本発明の一実施形態を図１乃至図３を参照して説明する。

【００３０】図１は本実施形態の暗号鍵の配送方法を適用する暗号通信システムの全体構成を示すものであり、鍵発行局に備えた端末装置１と各ユーザが所持する端末装置２とが、インターネット３を介して通信可能なように相互に接続されている。尚、各端末装置１，２とインターネット３との間にプロバイダのゲートウェイや公衆回線網等が介在してもよい。

【００３１】各端末装置１，２はパソコン等のコンピュータ（モデム等の通信機器やディスプレイ、キーボード等を含む）により構成されたもので、鍵発行局の端末装置１をサーバ、ユーザの端末装置２をクライアントとして端末装置１，２間でインターネット３を介して通信を行うために、鍵発行局の端末装置１には、周知のＴＣＰ／ＩＰ（Transmission Control Protocol ／Internet Protocol ）、ＨＴＴＰ（Hyper-Text Transfer Protocol）等のプロトコルがインターネット通信手段１ａとして組み込まれ、さらに、暗号通信システムへの加入申し込みのためのホームページが組み込まれている。

【００３２】また、ユーザの端末装置２には、ＴＣＰ／ＩＰや、ＨＴＴＰを含むブラウザがインターネット通信手段２ａとして組み込まれている。

【００３３】ここで、各端末装置１，２のインターネット通信手段１ａ，２ａに含まれるＨＴＴＰは、データの一回の通信が完結する毎に（１パケットの通信毎に）、インターネット３の不特定の通信経路を介して該データを通信する機能を有するものである。

【００３４】次に、この暗号通信システムにおいて、ユーザ同士が暗号通信を行うために必要な暗号鍵を鍵発行局から各ユーザに配送する際の作動を図２及び図３のフローチャートを参照して説明する。

【００３５】まず、暗号通信システムに加入しようとするユーザは、事前に鍵発行局（あるいはシステムの管理者）が配付するパスワードを取得しておく（ＳＴＥＰ１－１，２－１）。このパスワードは、例えば本実施形態の暗号通信システムがサポートしようとする地域以外のユーザを排除するためのものである。尚、このパスワードの各ユーザへの配付は、郵便等を通じてオフラインで行われる。

【００３６】次に、ユーザは、暗号通信システムに加入するとき、自身の端末装置２からインターネット通信手段２ａによってインターネット３を介して鍵発行局の端末装置１（サーバ）にアクセスする（ＳＴＥＰ１－２）。

【００３７】このとき、鍵発行局の端末装置１では、上記のようなアクセスがあると（ＳＴＥＰ２－２）、以下に説明するエルガマル暗号（Elgamal ）を用いた公開鍵方式による暗号通信を行うための公開鍵及び秘密鍵を生成して保持する（ＳＴＥＰ２－３）。

【００３８】上記エルガマル暗号では、ｐ：素数、ｋ：ｐ－１と互いに素である整数、ｇ：ｇ＜ｐである整数、ｘ：ｘ＜ｐである整数、ｙ：$y = g^x \bmod p$としたとき、通信データＭ（平文）を次式（１）により暗号化する。

【００３９】$b = y^k M \bmod p$　　……（１）

ここで、ｂは通信データＭを暗号化したものを示している。

【００４０】このように通信データＭを暗号化したと

き、ａ：ａ＝ｇ^ｋ mod ｐとすると、通信データＭは次式（２）により復号化される。

【００４１】Ｍ＝ｂ／ａ^ｘ mod ｐ　……（２）

そこで、本実施形態では、鍵発行局の端末装置１では、ＳＴＥＰ２－３において、前述のように定義された素数ｐ及び整数ｋ，ｇ，ｘを生成し、さらに前記ｙ（＝ｇ^ｘ mod ｐ）及びａ（＝ｇ^ｋ mod ｐ）を算出する。そして、これらのうち、ｙ，ｋ，ｐを通信データＭの暗号化のための公開鍵として保持し、ａ，ｘを素数ｐと併せて復号化のための秘密鍵として保持する。

【００４２】この場合、ＳＴＥＰ２－３では、前記公開鍵及び秘密鍵を規定する素数ｐ及び整数ｋ，ｇ，ｘをランダムに生成する。より具体的には、素数ｐの候補をあらかじめ複数用意しておき、ＳＴＥＰ２－３で公開鍵及び秘密鍵を生成するに際しては、用意した複数の素数の中から一つの素数ｐをランダムに選択する。そして、その選択した素数ｐに対して、整数ｋ，ｇ，ｘをそれぞれの前述の定義条件を満たすようにランダムに生成する。このとき、各素数ｐに対して整数ｋ，ｇ，ｘはそれぞれ有限個に定まるので、各素数ｐに対して整数ｋ，ｇ，ｘの候補をあらかじめ記憶保持しておき、それらの中から整数ｋ，ｇ，ｘを一つずつランダムに選択するようにしてもよい。

【００４３】尚、素数ｐは、前記式（１）により暗号化する通信データＭのサイズを例えば１バイト（２^８ ビット）としたとき、２^８ －１＝２５５以上の大きさのものを採用することが好ましい。

【００４４】上記のようにしてエルガマル暗号による公開鍵及び秘密鍵を生成して保持した後、鍵発行局の端末装置１（サーバ）は、ユーザの端末装置２（クライアント）に、該ユーザが暗号通信システムの加入申し込みをするためのホームページを前記インターネット通信手段１ａによってインターネット３を介してユーザの端末装置２に送信する（ＳＴＥＰ２－４）。

【００４５】このようにしてユーザがその端末装置２で上記ホームページを受信すると（ＳＴＥＰ１－３）、該ユーザは、上記ホームページに記載されている内容等を確認した後、前記公開鍵や、後述の処理のための必要な通信処理ソフトを該ユーザの端末装置２に受け取るためのダウンロード要求を、該端末装置２から前記インターネット通信手段２ａを介して鍵発行局の端末装置１に送信する（ＳＴＥＰ１－４）。

【００４６】このとき、鍵発行局の端末装置１では、上記ダウンロード要求を受信すると（ＳＴＥＰ２－５）、前記ＳＴＥＰ２－３で前述の如く生成した公開鍵（ｙ，ｋ，ｐ）とあらかじめ記憶保持している通信処理ソフトとをインターネット通信手段１ａを介してユーザの端末装置２に送信する（ＳＴＥＰ２－６）。

【００４７】ここで、上記通信処理ソフトには、後述の乱数データの生成のための処理ソフトや、暗号通信のための処理ソフト、ユーザの個人情報等の入力のための処理ソフト等が含まれている。

【００４８】このようにして、ユーザがその端末装置２に上記公開鍵及び通信処理ソフトを受信すると（ＳＴＥＰ１－５）、次に該ユーザの端末装置２では、前記通信処理ソフトが起動される（ＳＴＥＰ１－６）。

【００４９】このとき、該通信処理ソフトはまず、後述の共通鍵方式による暗号通信のためのセッションキーとして使用する乱数データを生成するためのモードとなり、このモードにおいて、以下に説明するように乱数データを生成して保存する（ＳＴＥＰ１－７）。

【００５０】すなわち、該通信処理ソフトは、端末装置２において、例えば所定の語句あるいは文章を入力させるようにユーザに指示する。このとき、その指示に従ってユーザが所定の語句あるいは文章を入力すると、通信処理ソフトはその語句あるいは文章の各単語間の入力の時間差を計測し、それらの時間差を種として乱数データ（セッションキー）を生成して保存する。この場合、この乱数データの種とする上記時間差はユーザの人為的操作によるものであるため、一般にユーザ毎に相違し、従って、生成される乱数データはユーザに固有のものとなる。また、各ユーザが前記語句あるいは文章の入力操作のタイミングを正確にコントロールすることも難しいので、今回限りの予測のつきにくい乱数データが生成される。

【００５１】このようにして乱数データを生成した後、通信処理ソフトはユーザの個人情報及びパスワードを該ユーザの端末装置２に入力させるモードとなり、このモードにおいて、ユーザは自身の個人情報と前記ＳＴＥＰ１－１で事前に取得しておいたパスワードとを端末装置２に入力する（ＳＴＥＰ１－８）。ここで、入力するユーザの個人情報は、該ユーザの住所、氏名、電話番号、電子メールアドレス等である。

【００５２】このようにしてユーザの個人情報及びパスワードが入力されると、通信処理ソフトは、次に前記ＳＴＥＰ１－７で生成した乱数データ（セッションキー）とＳＴＥＰ１－８で入力されたユーザの個人情報及びパスワードとを、前記ＳＴＥＰ１－５で端末装置２にダウンロードされた公開鍵を用いて前記式（１）により暗号化する（ＳＴＥＰ１－９）。そして、通信処理ソフトは、このように暗号化した乱数データ（セッションキー）、個人情報及びパスワードを端末装置２のインターネット通信手段２ａを介して鍵発行局の端末装置１に送信する（ＳＴＥＰ１－１０）。

【００５３】一方、鍵発行局の端末装置１では、上記のように公開鍵によって暗号化された乱数データ、個人情報及びパスワードを受信すると（ＳＴＥＰ２－７）、前記ＳＴＥＰ２－３で前述の如く生成して保持した秘密鍵（ａ，ｘ，ｐ）を用いて、前記式（２）により上記の暗号化データを復号化し、これにより乱数データ、個人情

報及びパスワードを取得する（ＳＴＥＰ２－８）。このとき、乱数データが、ユーザの端末装置２及び鍵発行局の端末装置１の両者において、後述する共通鍵方式による暗号通信のための共通のセッションキーとして所持されることとなる。

【００５４】次いで、鍵発行局の端末装置１では、前記ＳＴＥＰ２－１でユーザにパスワードを配付する際にユーザ側から取得していたユーザの情報や、ＳＴＥＰ２－８で取得した個人情報の照合等を行うことで、ＳＴＥＰ２－８で取得したパスワードを確認し（ＳＴＥＰ２－９）、パスワードが正しければ、ＳＴＥＰ２－８で取得した個人情報を端末装置１のデータベースに登録する（ＳＴＥＰ２－１０）。また、パスワードが正しくなければＳＴＥＰ２－３からの処理に戻って、公開鍵及び秘密鍵を新たにに生成し直すと共に、ホームページをユーザの端末装置２に送信する。尚、この場合、鍵発行局の端末装置１は、パスワードが間違っている旨のメッセージや、ユーザの前述したような手続き処理をやり直すように要求する旨のメッセージをホームページと併せてユーザの端末装置２に送信する。

【００５５】上記のようにユーザの個人情報を登録した後、鍵発行局の端末装置１では、その登録したユーザが、後に他のユーザとの間で暗号通信を行うための個人鍵（暗号鍵）を生成する（ＳＴＥＰ２－１１）。

【００５６】ここで、本実施形態の暗号通信システムでは、ユーザ同士の暗号通信の方式として共通鍵方式を採用しており、上記ＳＴＥＰ２－１１で生成する個人鍵は、ユーザ同士が暗号通信を行う際に、そのユーザ同士が互いに共有する共通鍵を生成するためのアルゴリズムにより構成されるものである。より詳しくは、このアルゴリズムは、ユーザ同士の暗号通信に際して、それぞれのユーザが自身の端末装置２で該アルゴリズムに対して通信相手側の氏名等の識別子を入力することで、その通信相手側のユーザとの暗号通信のための共通鍵を生成するものである。そして、鍵発行局の端末装置１では、このような個人鍵（アルゴリズム）をＳＴＥＰ２－８で取得した個人情報や乱数データに基づいて生成する。

【００５７】尚、このような個人鍵のより具体的な生成手法は、本願出願人が例えば特願平９－２３７４５号にて詳細に説明しているので、ここではさらなる説明を省略する。

【００５８】上記のようにユーザの個人鍵（暗号鍵）を生成した後、鍵発行局の端末装置１は、ＳＴＥＰ２－８で取得した乱数データを共通鍵方式の暗号通信による個人鍵の配送のためのセッションキー（これはユーザ同士で暗号通信を行うための共通鍵とは異なることに注意）として用いて、ＳＴＥＰ２－１１で生成した個人鍵を暗号化する（ＳＴＥＰ２－１２）。この場合、この暗号化は、例えば３段構成のＤＥＳ（Data Encryption Standard）により行われる。

【００５９】そして、鍵発行局の端末装置１は、このように暗号化した個人鍵をインターネット通信手段１ａを介してユーザの端末装置２に送信する（ＳＴＥＰ２－１３）。

【００６０】一方、上記のように暗号化された個人鍵は、ユーザの端末装置２によって受信される（ＳＴＥＰ１－１１）。そして、暗号化された個人鍵を受信したユーザの端末装置２では、前記通信処理ソフトによって、前記ＳＴＥＰ１－７で生成・保持した乱数データをセッションキーとして用いて該個人鍵が復号化され、端末装置２に保存される（ＳＴＥＰ１－１２）。

【００６１】以上により、鍵発行局からユーザへの個人鍵（暗号鍵）の配送が完了する。以後は、この個人鍵を受け取ったユーザは、他のユーザと暗号通信をする際に、自身の端末装置２に保存した個人鍵に通信相手側のユーザの識別子（氏名等）を該端末装置２上で作用させることにより、通信相手側のユーザとの共通鍵を生成する。そして、その共通鍵を用いてユーザ同士の暗号通信が行われることとなる。

【００６２】本実施形態における個人鍵（暗号鍵）の各ユーザへの配送手法によれば、前述の如く、まず、鍵発行局の端末装置１からユーザの端末装置２にエルガマル暗号による公開鍵がインターネット３を介して与えられ、さらにユーザ側の端末装置２で生成した乱数データやユーザの個人情報等が該公開鍵によって暗号化された後、ユーザの端末装置２から鍵発行局の端末装置１に与えられる。そして、この暗号化された乱数データやユーザの個人情報を鍵発行局の端末装置１で前記公開鍵に対応する秘密鍵によって復号化することで、鍵発行局側がユーザ側の所持する乱数データと同じ乱数データを共有すると共に、該ユーザの個人情報を取得する。このような通信において、鍵発行局側からユーザ側への公開鍵の通信や、この公開鍵により暗号化された乱数データ、個人情報等のユーザ側から鍵発行局側への通信は、前記ＨＴＴＰを有するインターネット通信手段１ａ，１ｂを介して行われるため、それらの通信は一般にはインターネット３上の異なる通信経路を経由して行われる。このため、前記公開鍵や、この公開鍵により暗号化された乱数データ、個人情報等を第三者が個別に獲得することがあっても、それらをひとまとめに関連付けて獲得することは難しい。しかも、前記公開鍵や秘密鍵は、何度の繰り返し用いられるものではなく、公開鍵の送信を行う毎にランダムに生成され、基本的には、その都度、異なるものが生成される。そして、ユーザ側から鍵発行局側に受け渡される乱数データや個人情報は、このような公開鍵によって暗号化されたものである。

【００６３】従って、ユーザ側から鍵発行局側への乱数データや個人情報のインターネット３を介した受け渡しに際して、第三者が、暗号化された乱数データや個人情報を獲得しても、該乱数データや個人情報を解読するこ

とは困難である。特に、鍵発行局側からユーザ側への前記個人鍵の最終的な配送の際のセッションキーとして使用する乱数データは元々、ユーザの人為的な端末装置２の入力操作に基づいて生成された予測のつきにくいものであるため、該乱数データの解読の困難性が高いものとなる。

【００６４】この場合、この乱数データや個人情報の暗号通信の基礎となる前記エルガマル暗号は、これと同じ公開鍵方式の範疇に属するＲＳＡに較べて安全性の強度が弱いとされているものの、上記のような理由によって、十分に安全性を確保することができる。また、本実施形態で使用するエルガマル暗号は、ＲＳＡに較べて暗号化や複合化のための処理が簡単で、該処理を効率よく短時間で行うことができる。

【００６５】以上のように本実施形態では、鍵発行局側からユーザ側への前記個人鍵を配送する前に、ユーザ側から鍵発行局側に行われる乱数データや個人情報の通信を安全且つ効率よく行うことができ、特に、個人鍵の暗号通信による配送の際にセッションキーとして使用する乱数データを第三者によって解読されたりすることなく、ユーザ側と鍵発行局側とで安全に共有することができる。

【００６６】また、本実施形態の個人鍵（暗号鍵）の各ユーザへの配送手法によれば、上記のように乱数データがユーザ側と鍵発行局側とで共有された後には、該乱数データを共通鍵方式によるセッションキー（共通鍵）として使用して、鍵発行局側で生成した個人鍵（暗号鍵）が暗号化されてユーザ側にインターネット３を介して与えられる。そして、ユーザ側では、その暗号化された個人鍵を、前記乱数データをセッションキーとして使用して復号化することで取得する。

【００６７】このとき、前記公開鍵や、これにより暗号化された乱数データ等の通信の場合と同様に、前記乱数データ（セッションキー）によって暗号化された個人鍵の通信は、前記ＨＴＴＰを有するインターネット通信手段１ａ，１ｂを介して行われるため、それらの通信データを第三者がひとまとめに獲得することは難しく、しかも、上記乱数データをセッションキーとして使用する共通鍵方式による暗号通信は、鍵発行局側からユーザ側に個人鍵を配送する時のただ一度だけである。また、この暗号通信のセッションキーである乱数データは前述の通り予測のつきにくいものである。

【００６８】従って、鍵発行局側からユーザ側への最終的な個人鍵（暗号鍵）のインターネット３を介した受け渡しに際して、第三者が、暗号化された個人鍵を獲得しても、該個人鍵を解読することは極めて困難である。

【００６９】また、最終的な個人鍵の配送は公開鍵方式に比して暗号化や複合化の処理が容易な共通鍵方式であるため、該個人鍵の配送を迅速に効率よく行うことができる。

【００７０】このように本実施形態の個人鍵（暗号鍵）の配送手法によれば、インターネット３を使用した通信によって、安全且つ簡単に、しかも短い時間で鍵発行局から各ユーザに、ユーザ同士の暗号通信のために必要な個人鍵を受け渡すことができ、汎用性や利便性に優れた暗号通信システムを構築することができる。

【００７１】尚、本実施形態では、公開鍵方式による乱数データ（セッションキー）の暗号通信に際して、エルガマル暗号を用いたが、ＲＳＡ暗号を用いてもよいことはもちろんである。但し、前述したようにエルガマル暗号を使用しても、十分な安全性を確保することができ、また、ＲＳＡ暗号よりもエルガマル暗号の方が、暗号化や復号化の処理を効率よく短時間で行うことができるため、エルガマル暗号を使用した方が、システム処理の迅速性や簡易性の点で有利である。

【００７２】また、本実施形態では、個人鍵（暗号鍵）の配送処理と併せてユーザの個人情報の授受を行うようにしたが、ユーザの個人情報の授受は事前に別途、行っておき、その後に個人鍵（暗号鍵）の配送処理のみを本実施形態と同様に行うようにしてもよい。

【図面の簡単な説明】

【図１】本発明の一実施形態の暗号鍵の配送方法を適用する暗号通信システムの全体構成を示す図。

【図２】図１のシステムにおける暗号鍵の配送方法を説明するためのフローチャート。

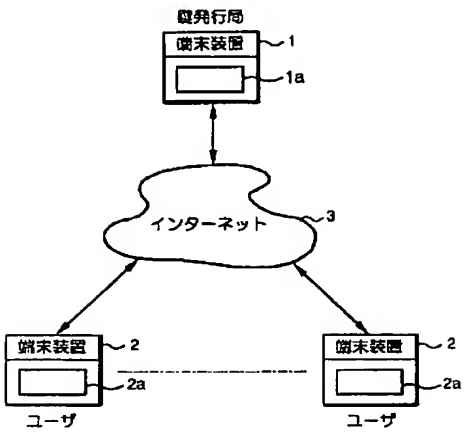
【図３】図１のシステムにおける暗号鍵の配送方法を説明するためのフローチャート。

【符号の説明】

１…鍵発行局の端末装置、２…ユーザの端末装置、１ａ，２ａ…インターネット通信手段、３…インターネット。

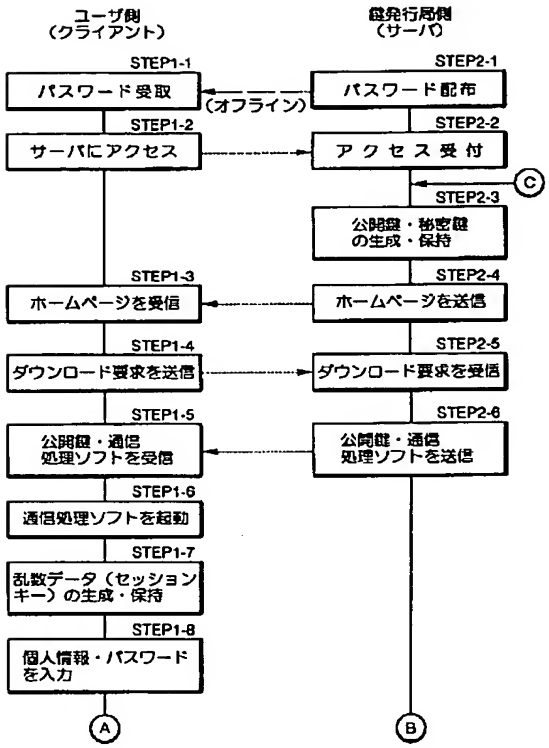
【図１】

FIG. 1



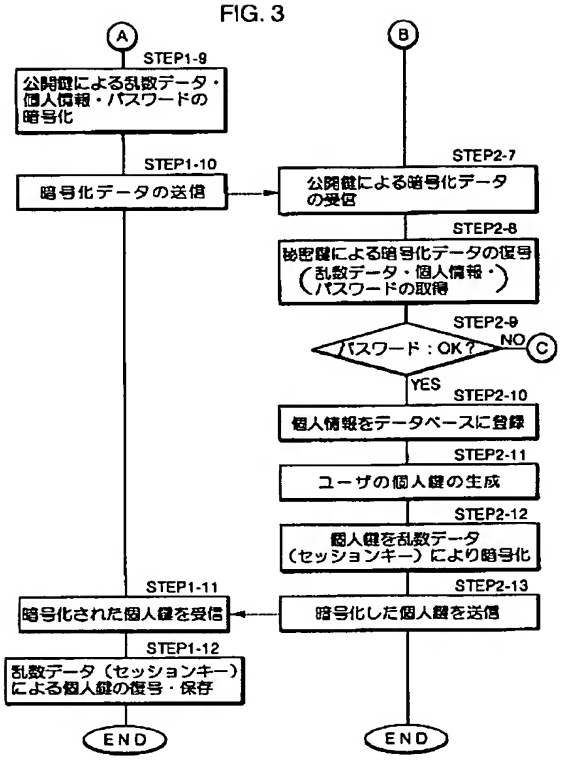
【図２】

FIG. 2



【図３】

FIG. 3


A
B
STEP1-9
公開鍵による乱数データ・個人情報・パスワードの暗号化
STEP1-10
暗号化データの送信
STEP2-7
公開鍵による暗号化データの受信
STEP2-8
秘密鍵による暗号化データの復号（乱数データ・個人情報・）パスワードの取得
STEP2-9
パスワード：OK？
NO
C
YES
STEP2-10
個人情報をデータベースに登録
STEP2-11
ユーザの個人鍵の生成
STEP2-12
個人鍵を乱数データ（セッションキー）により暗号化
STEP2-13
暗号化した個人鍵を送信
STEP1-11
暗号化された個人鍵を受信
STEP1-12
乱数データ（セッションキー）による個人鍵の復号・保存
END
END